IT Security Definitions as of October 31, 2003

NOTE: If you can't find the term here, go to:

http://www.itsecurity.com/dictionary/dictionary.htm

Acceptable Risk is a concern that is acceptable to responsible management, due to the cost and magnitude of implementing controls / countermeasures..

Accreditation is synonymous with the term authorize processing. Accreditation is the authorization and approval granted to a major application or general support system to process in an operational environment. It is made on the basis of a certification by designated technical personnel that the system meets pre-specified technical requirements for achieving adequate system security. See also ***Authorize Processing, Certification*** and ***Designated Approving Authority.***

Active Attack

An attack which results in an unauthorized state change, such as the manipulation of files, or the adding of unauthorized files

Adequate Security**.** Security implemented to fully meet the requirements put forth in public laws, Executive Branch directions, Federal standards, and agency-specific policies. Security will be implemented commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the Department operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost effective management, personnel, operational, and technical controls.

Administrative Security

The management constraints and supplemental controls established to provide an acceptable level of protection for data.

AIS

Automated Information System - any equipment of an interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, control, display, transmission, or reception of data and includes software, firmware, and hardware.

Alert

A formatted message describing a circumstance relevant to network security. Alerts are often derived from critical audit events. Ankle-Biter

A person who aspires to be a hacker/cracker but has very limited knowledge or skills related to AIS's. Usually associated with young teens who collect and use simple malicious programs obtained from the Internet.

Anomaly Detection Model

A model where intrusions are detected by looking for activity that is different from the user's or system's normal behavior.

Application Level Gateway

(Firewall) A firewall system in which service is provided by processes that maintain complete TCP connection state and sequencing. Application level firewalls often re-address traffic so that outgoing traffic appears to have originated from the firewall, rather than the internal host.

ASIM

Automated Security Incident Measurement - Monitors network traffic and collects information on targeted unit networks by detecting unauthorized network activity.

Asset is a major application, general support system, high impact program, physical plant, mission critical system, or a logically related group of systems.

Assessment

Surveys and Inspections; an analysis of the vulnerabilities of an AIS. Information acquisition and review process designed to assist a customer to determine how best to use resources to protect information in systems.

Assurance

A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy.

Attack

An attempt to bypass security controls on a computer. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.

Audit

The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

Audit Trail

In computer security systems, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.

Authenticate

To establish the validity of a claimed user or object.

Authentication

To positively verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

Authentication Header (AH)

A field that immediately follows the IP header in an IP datagram and provides authentication and integrity checking for the datagram.

Authorize Processing, Certification, and Designated Approving Authority. Authorize Processing occurs when management authorizes in writing a system based on an assessment of management, operational, and technical controls. By authorizing processing in a system the management official accepts the risks associated with it. See also ***Accreditation, Certification,*** and ***Designated Approving Authority.***

Automatic Data Processing (ADP) System - An assembly of computer hardware, firmware, and software configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, storing, and retrieving data with a minimum of human intervention.

Availability. Protection requires backup of system and information, contingency plans, disaster recovery plans, and redundancy. Examples of systems and information requiring availability protection are time-share systems, mission-critical applications, time and attendance, financial, procurement, or life-critical. ***Availability:*** A "requirement intended to assure that systems work promptly and service is not denied to authorized users".

Awareness, Training, and Education includes (1) awareness programs set the stage for training by changing organizational attitudes towards realization of the importance of security and the adverse consequences of its failure; (2) the purpose of training is to teach people the skills that will enable them to perform their jobs more effectively; and (3) education is more in-depth than training and is targeted for security professionals and those whose jobs require expertise in IT security.

Automated Security Monitoring

All security features needed to provide an acceptable level of protection for hardware, software, and classified, sensitive, unclassified or critical data, material, or processes in the system.

Availability

Assuring information and communications services will be ready for use when expected.

[B]

Back Door

A hole in the security of a computer system deliberately left in place by designers or maintainers. Synonymous with trap door; a hidden software or hardware mechanism used to circumvent security controls.

Bell-La Padula Security Model

Formal-state transition model of computer security policy that describes a formal set of access controls based on information sensitivity and subject authorizations.

Biba Integrity Model

A formal security model for the integrity of subjects and objects in a system.

Bomb

A general synonym for crash, normally of software or operating system failures.

Breach

The successful defeat of security controls which could result in a penetration of the system. A violation of controls of a particular information system such that information assets or system components are unduly exposed.

Buffer Overflow

This happens when more data is put into a buffer or holding area than the buffer can handle. This is due to a mismatch in processing rates between the producing and consuming processes. This can result in system crashes or the creation of a back door leading to system access.

Bug

An unwanted and unintended property of a program or piece of hardware, especially one that causes it to malfunction.

[C]

C2

Command and Control

C2-attack

Prevent effective C2 of adversary forces by denying information to, influencing, degrading or destroying the adversary C2 system.

C2-protect

Maintain effective command and control of own forces by turning to friendly advantage or negating adversary effort to deny information to, influence, degrade, or destroy the friendly C2 system. (Pending approval in JP 1-02)

CGI

Common Gateway Interface - CGI is the method that Web servers use to allow interaction between servers and programs.

CGI Scripts

Allows for the creation of dynamic and interactive web pages. They also tend to be the most vulnerable part of a web server (besides the underlying host security).

Check_Password

A hacking program used for cracking VMS passwords.

Chernobyl Packet

Also called Kamikaze Packet. A network packet that induces a broadcast storm and network meltdown. Typically an IP Ethernet datagram that passes through a gateway with both source and destination Ethernet and IP address set as the respective broadcast addresses for the subnetworks being gated between.

Circuit Level Gateway

One form of a firewall. Validates TCP and UDP sessions before opening a connection. Creates a handshake, and once that takes place passes everything through until the session is ended.

Clipper chip

A tamper-resistant VLSI chip designed by NSA for encrypting voice communications. It conforms to the Escrow Encryption Standard (EES) and implements the Skipjack encryption algorithm.

COAST

Computer Operations, Audit, and Security Technology - is a multiple project, multiple investigator laboratory in computer security research in the Computer Sciences Department at Purdue University. It functions with close ties to researchers and engineers in major companies and government agencies. Its research is focused on real-world needs and limitations, with a special focus on security for legacy computing systems.

Command and Control Warfare

(C2W) The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare is an application of information operations in military operations and is a subset of information warfare. C2W is both offensive and defensive.

Compromise

An intrusion into a computer system where unauthorized disclosure, modification or destruction of sensitive information may have occurred

Computer Abuse

The willful or negligent unauthorized activity that affects the availability, confidentiality, or integrity of computer resources. Computer abuse includes fraud, embezzlement, theft, malicious damage, unauthorized use, denial of service, and misappropriation.

Computer Fraud

Computer-related crimes involving deliberate misrepresentation or alteration of data in order to obtain something of value.

Computer Network Attack

(CNA) Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (DODD S-3600.1 of 9 Dec 96)

Computer Security

Technological and managerial procedures applied to computer systems to ensure the availability, integrity and confidentiality of information managed by the computer system.

Computer Security Incident

Any intrusion or attempted intrusion into an automated information system (AIS). Incidents can include probes of multiple computer systems.

Computer Security Intrusion

Any event of unauthorized access or penetration to an automated information system (AIS).

Confidentiality

Assuring information will be kept secret, with access limited to appropriate persons.

COPS

Computer Oracle and Password System - A computer network monitoring system for Unix machines. Software tool for checking security on shell scripts and C programs. Checks for security weaknesses and provides warnings.

COTS Software

Commercial Off the Shelf - Software acquired by government contract through a commercial vendor. This software is a standard product, not developed by a vendor for a particular government project.

Countermeasures

Action, device, procedure, technique, or other measure that reduces the vulnerability of an automated information system. Countermeasures that are aimed at specific threats and vulnerabilities involve more sophisticated techniques as well as activities traditionally perceived as security.

Crack

A popular hacking tool used to decode encrypted passwords. System administrators also use Crack to assess weak passwords by novice users in order to enhance the security of the AIS.

Cracker

One who breaks security on an AIS.

Cracking

The act of breaking into a computer system.

Crash

A sudden, usually drastic failure of a computer system.

Cryptanalysis

Definition 1) The analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data including cleartext.

Definition 2) Operations performed in converting encrypted messages to plain text without initial knowledge of the crypto-algorithm and/or key employed in the encryption.

Cryptographic Hash Function

A process that computes a value (referred to as a hashword) from a particular data unit in a manner that, when a hashword is protected, manipulation of the data is detectable.

Cryptography

The art of science concerning the principles, means, and methods for rendering plain text unintelligible and for converting encrypted messages into intelligible form.

Cryptology

The science which deals with hidden, disguised, or encrypted communications.

Cyberspace

Describes the world of connected computers and the society that gathers around them. Commonly known as the INTERNET.

[D]

Dark-side Hacker

A criminal or malicious hacker.

DARPA

Defense Advanced Research Projects Agency.

Data Driven Attack

A form of attack that is encoded in innocuous seeming data which is executed by a user or a process to implement an attack. A data driven attack is a concern for firewalls, since it may get through the firewall in data form and launch an attack against a system behind the firewall.

Data Encryption Standard

Definition 1) (DES) An unclassified crypto algorithm adopted by the National Bureau of Standards for public use.

Definition 2) A cryptographic algorithm for the protection of unclassified data, published in Federal Information Processing Standard (FIPS) 46. The DES, which was approved by the National Institute of Standards and Technology (NIST), is intended for public and government use.

Defense Information Infrastructure (DII)

The shared or interconnected system of computers, communications, data applications, security, people, training and other support structures serving DoD local, national, and worldwide information needs. DII connects DoD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to the subscribers over the Defense Information Systems Network and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DoD information. (Pending approval in JP 1-02)

Defensive Information Operations

A process that integrates and coordinates policies and procedures, operations, personnel, and technology to protect information and defend information systems. Defensive information operations are conducted through information assurance, physical security, operations security, counter-deception, counter-psychological operations, counter-intelligence, electronic protect, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. (Pending approval in JP 1-02)

Demon Dialer

A program which repeatedly calls the same telephone number. This is benign and legitimate for access to a BBS or malicious when used as a denial of service attack.

Denial of Service

Action(s) which prevent any part of an AIS from functioning in accordance with its intended purpose.

Derf

The act of exploiting a terminal which someone else has absent mindedly left logged on.

DES

See Data Encryption Standard

DNS Spoofing

Assuming the DNS name of another system by either corrupting the name service cache of a victim system, or by compromising a domain name server for a valid domain.

[E]

Electronic Attack (EA)

That division of EW involving the use of electromagnetic, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. EA includes: actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception and employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency, particle beams).

Electronic Protection (EP)

That division of EW involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of EW that degrade, neutralize, or destroy friendly combat capability.

Electronic Warfare (EW)

Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are electronic attack, electronic protection, and electronic warfare support.

Electronic Warfare Support (ES)

That division of EW involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions involving EW operations and other tactical actions such as threat avoidance, targeting and homing. ES data can be used to produce signals intelligence. (JP 1-02)

Encapsulating Security Payload (ESA)

A mechanism to provide confidentiality and integrity protection to IP datagrams.

Ethernet Sniffing

This is listening with software to the Ethernet interface for packets that interest the user. When the software sees a packet that fits certain criteria, it logs it to a file. The most common criteria for an interesting packet is one that contains words like login or password.

[F]

False Negative

Occurs when an actual intrusive action has occurred but the system allows it to pass as non-intrusive behavior.

False Positive

Occurs when the system classifies an action as anomalous (a possible intrusion) when it is a legitimate action.

Fault Tolerance

The ability of a system or component to continue normal operation despite the presence of hardware or software faults.

Firewall

A system or combination of systems that enforces a boundary between two or more networks. Gateway that limits access between networks in accordance with local security policy. The typical firewall is an inexpensive micro-based Unix box kept clean of critical data, with many modems and public network ports on it, but just one carefully watched connection back to the rest of the cluster.

Fishbowl

To contain, isolate and monitor an unauthorized user within a system in order to gain information about the user.

Fork Bomb

Also known as Logic Bomb - Code that can be written in one line of code on any Unix system; used to recursively spawn copies of itself, "explodes" eventually eating all the process table entries and effectively locks up the system.

[H]

Hacker

A person who enjoys exploring the details of computers and how to stretch their capabilities. A malicious or inquisitive meddler who tries to discover information by poking around. A person who enjoys learning the details of programming systems and how to stretch their capabilities, as opposed to most users who prefer to learn on the minimum necessary.

Hacking

Unauthorized use, or attempts to circumvent or bypass the security mechanisms of an information system or network.

Hacking Run

A hack session extended long outside normal working times, especially one longer than 12 hours.

Host

A single computer or workstation; it can be connected to a network

Host Based

Information, such as audit data from a single host which may be used to detect intrusions

[I]

IDEA

(International Data Encryption Algorithm) - A private key encryption-decryption algorithm that uses a key that is twice the length of a DES key.

IDIOT

Intrusion Detection In Our Time. A system that detects intrusions using pattern-matching.

Information Assurance (IA)

Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DODD S-3600.1 of 9 Dec 96)

Information Operations (IO)

Actions taken to affect adversary information and information systems while defending one's own information and information systems. (DODD S-3600.1 of 9 Dec 96)

Information Security

The result of any system of policies and/or procedures for identifying, controlling, and protecting from unauthorized disclosure, information whose protection is authorized by executive order or statute.

Information Superiority

The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (DODD S-3600.1 of 9 Dec 96)

Information Warfare

Actions taken to achieve information superiority by affecting adversary information, information based processes, and information systems, while defending our own information, information based processes, and information systems. Any action to deny, exploit, corrupt, or destroy the enemy's information and its functions, protect themselves against those actions; and exploiting their own military information functions.

Information Warfare (IW)

Information Operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. (DODD S-3600.1 of 9 Dec 96)

Integrity

Assuring information will not be accidentally or maliciously altered or destroyed.

Internet Worm

A worm program (see: Worm) that was unleashed on the Internet in 1988. It was written by Robert T. Morris as an experiment that got out of hand.

Intrusion

Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.

Intrusion Detection

Pertaining to techniques which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.

IP Splicing / Hijacking

An action whereby an active, established, session is intercepted and co-opted by the unauthorized user. IP splicing attacks may occur after an authentication has been made, permitting the attacker to assume the role of an already authorized user. Primary protections against IP splicing rely on encryption at the session or network layer.

IP Spoofing

An attack whereby a system attempts to illicitly impersonate another system by using IP network address.

[K]

Key

A symbol or sequence of symbols (or electrical or mechanical correlates of symbols) applied to text in order to encrypt or decrypt

Key Escrow

The system of giving a piece of a key to each of a certain number of trustees such that the key can be recovered with the collaboration of all the trustees.

Keystroke Monitoring

A specialized form of audit trail software, or a specially designed device, that records every key struck by a user and every character of the response that the AIS returns to the user.

[L]

LAN

Local Area Network - A computer communications system limited to no more than a few miles and using high-speed connections (2 to 100 megabits per second). A short-haul communications system that connects ADP devices in a building or group of buildings within a few square kilometers, including workstations, front-end processors, controllers, switches, and gateways.

Leapfrog Attack

Use of userid and password information obtained illicitly from one host to compromise another host. The act of TELNETing through one or more hosts in order to preclude a trace (a standard cracker procedure).

Letterbomb

A piece of email containing live data intended to do malicious things to the recipient's machine or terminal. Under UNIX, a letterbomb can also try to get part of its contents interpreted as a shell command to the mailer. The results of this could range from silly to denial of service.

Logic Bomb

Also known as a Fork Bomb - A resident computer program which, when executed, checks for a particular condition or particular state of the system which, when satisfied, triggers the perpetration of an unauthorized act

[M]

Mailbomb

The mail sent to urge others to send massive amounts of email to a single system or person, with the intent to crash the recipient's system. Mailbombing is widely regarded as a serious offense.

Malicious Code

Hardware, software, of firmware that is intentionally included in a system for an unauthorized purpose; e.g. a Trojan horse

Metric

A random variable x representing a quantitative measure accumulated over a period.

Mimicking

Synonymous with Impersonation, Masquerading or Spoofing.

Misuse Detection Model

The system detects intrusions by looking for activity that corresponds to a known intrusion techniques or system vulnerabilities. Also known as Rules Based detection.

Mockingbird

A computer program or process which mimics the legitimate behavior of a normal system feature (or other apparently useful function) but performs malicious activities once invoked by the user.

Multihost Based Auditing

Audit data from multiple hosts may be used to detect intrusions.

[N]

Nak Attack

Negative Acknowledgment - A penetration technique which capitalizes on a potential weakness in an operating system that does not handle asynchronous interrupts properly and thus, leaves the system in an unprotected state during such interrupts.

National Computer Security Center (NCSC)

Originally named the DoD Computer Security Center, the NCSC is responsible for encouraging the widespread availability of trusted computer systems throughout the Federal Government. (AF9K_JBC.TXT) (NCSC) With the signing of NSDD-145; the NCSC is responsible for encouraging the widespread availability of trusted computer systems throughout the Federal Government. (NCSC-WA-001-85)

National Information Infrastructure (NII)

The nation-wide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The NII encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, monitors, printers and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the NII. (Pending approval in JP 1-02)

NCSC

See National Computer Security Center

Network

Two or more machines interconnected for communications.

Network Based

Network traffic data along with audit data from the hosts used to detect intrusions.

Network Level Firewall

A firewall in which traffic is examined at the network protocol (IP) packet level.

Network Security

Protection of networks and their services from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side-effects. Network security includes providing for data integrity.

Network Security Officer

Individual formally appointed by a designated approving authority to ensure that the provisions of all applicable directives are implemented throughout the life cycle of an automated information system network.

Network Weaving

Another name for "Leapfrogging"

Non-Discretionary Security

The aspect of DOD security policy which restricts access on the basis of security levels. A security level is composed of a read level and a category set restriction. For read-access to an item of information, a user must have a clearance level greater then or equal to the classification of the information and also have a category clearance which includes all of the access categories specified for the information.

Non-Repudiation

Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.

[O]

Open Security

Environment that does not provide environment sufficient assurance that applications and equipment are protected against the introduction of malicious logic prior to or during the operation of a system.

Open Systems Security

Provision of tools for the secure internetworking of open systems.

Operational Data Security

The protection of data from either accidental or unauthorized, intentional modification, destruction, or disclosure during input, processing, or output operations.

Operations Security

Definition 1) The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities.

Definition 2) An analytical process by with the U.S. Government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting evidence of the planning and execution of sensitive activities and operations.

Operations Security (OPSEC)

A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. Identify those actions that can be observed by adversary intelligence systems. b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. (JP 1-02)

Orange Book

See Trusted Computer Security Evaluation Criteria

OSI

Open Systems Interconnection. A set of internationally accepted and openly developed standards that meet the needs of network resource administration and integrated network utility.

[P]

Packet

A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.

Packet Filter

Inspects each packet for user defined content, such as an IP address but does not track the state of sessions. This is one of the least secure types of firewall.

Packet Filtering

A feature incorporated into routers and bridges to limit the flow of information based on pre-determined communications such as source, destination, or type of service being provided by the network. Packet filters let the administrator limit protocol specific traffic to one network segment, isolate email domains, and perform many other traffic control functions.

Packet Sniffer

A device or program that monitors the data traveling between computers on a network

Passive Attack

Attack which does not result in an unauthorized state change, such as an attack that only monitors and/or records data.

Passive Threat

The threat of unauthorized disclosure of information without changing the state of the system. A type of threat that involves the interception, not the alteration, of information.

PEM (Privacy Enhanced Mail)

An IETF standard for secure electronic mail exchange.

Penetration

The successful unauthorized access to an automated system.

Penetration Signature

The description of a situation or set of conditions in which a penetration could occur or of system events which in conjunction can indicate the occurrence of a penetration in progress.

Penetration Testing

The portion of security testing in which the evaluators attempt to circumvent the security features of a system. The evaluators may be assumed to use all system design and implementation documentation, that may include listings of system source code, manuals, and circuit diagrams. The evaluators work under the same constraints applied to ordinary users.

Perimeter Based Security

The technique of securing a network by controlling access to all entry and exit points of the network. Usually associated with firewalls and/or filters.

Perpetrator

The entity from the external environment that is taken to be the cause of a risk. An entity in the external environment that performs an attack, i.e. hacker.

Personnel Security

The procedures established to ensure that all personnel who have access to any classified information have the required authorizations as well as the appropriate clearances.

PGP (Pretty Good Privacy)

A freeware program primarily for secure electronic mail.

Phage

A program that modifies other programs or databases in unauthorized ways; especially one that propagates a virus or Trojan horse.

PHF

Phone book file demonstration program that hackers use to gain access to a computer system and potentially read and capture password files.

PHF hack

A well-known and vulnerable CGI script which does not filter out special characters (such as a new line) input by a user.

Phracker

An individual who combines phone phreaking with computer hacking.

Phreak(er)

An individual fascinated by the telephone system. Commonly, an individual who uses his knowledge of the telephone system to make calls at the expense of another.

Phreaking

The art and science of cracking the phone network.

Physical Security

The measures used to provide physical protection of resources against deliberate and accidental threats.

Piggy Back

The gaining of unauthorized access to a system via another user's legitimate connection.

Ping of Death

The use of Ping with a packet size higher than 65,507. This will cause a denial of service.

Plaintext

Unencrypted data.

Private Key Cryptography

An encryption methodology in which the encryptor and decryptor use the same key, which must be kept secret. This methodology is usually only used by a small group.

Probe

Any effort to gather information about a machine or its users for the apparent purpose of gaining unauthorized access to the system at a later date.

Procedural Security

See Administrative Security.

Profile

Patterns of a user's activity which can detect changes in normal routines.

Promiscuous Mode

Normally an Ethernet interface reads all address information and accepts follow-on packets only destined for itself, but when the interface is in promiscuous mode, it reads all information (sniffer), regardless of its destination.

Protocol

Agreed-upon methods of communications used by computers. A specification that describes the rules and procedures that products should follow to perform activities on a network, such as transmitting data. If they use the same protocols, products from different vendors should be able to communicate on the same network.

Prowler

A daemon that is run periodically to seek out and erase core files, truncate administrative logfiles, nuke lost+found directories, and otherwise clean up.

Proxy

A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it. A software agent that acts on behalf of a user, typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination.

Psychological Operations (PSYOP)

Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. (JP 1-02)

Public Key Cryptography

Type of cryptography in which the encryption process is publicly available and unprotected, but in which a part of the decryption key is protected so that only a party with knowledge of both parts of the decryption process can decrypt the cipher text.

[R]

Red Book

See Trusted Network Interpretation.

Reference Monitor

A security control concept in which an abstract machine mediates accesses to objects by subjects. In principle, a reference monitor should be complete (in that it mediates every access), isolated from modification by system entities, and verifiable. A security kernel is an implementation of a reference monitor for a given hardware base.

Replicator

Any program that acts to produce copies of itself examples include; a program, a worm, a fork bomb or virus. It is even claimed by some that UNIX and C are the symbiotic halves of an extremely successful replicator.

Retro-Virus

A retro-virus is a virus that waits until all possible backup media are infected too, so that it is not possible to restore the system to an uninfected state.

Rexd

This Unix command is the Sun RPC server for remote program execution. This daemon is started by inetd whenever a remote execution request is made.

Risk Assessment

A study of vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of security measures. The process of evaluating threats and vulnerabilities, known and postulated, to determine expected loss and establish the degree of acceptability to system operations.

Risk Management

The total process to identify, control, and minimize the impact of uncertain events. The objective of the risk management program is to reduce risk and obtain and maintain DAA (Designated Approving Authority) approval.

Rootkit

A hacker security tool that captures passwords and message traffic to and from a computer. A collection of tools that allows a hacker to provide a backdoor into a system, collect information on other systems on the network, mask the fact that the system is compromised, and much more. Rootkit is a classic example of

Trojan Horse software. Rootkit is available for a wide range of operating systems.

Router

An interconnection device that is similar to a bridge but serves packets or frames containing certain protocols. Routers link LANs at the network layer.

Routing Control

The application of rules during the process of routing so as to choose or avoid specific networks, links or relays.

RSA Algorithm

RSA stands for Rivest-Shamir-Aldeman. A public-key cryptographic algorithm that hinges on the assumption that the factoring of the product of two large primes is difficult.

Rules Based Detection

The intrusion detection system detects intrusions by looking for activity that corresponds to known intrusion techniques (signatures) or system vulnerabilities. Also known as Misuse Detection.

[S] Samurai

A hacker who hires out for legal cracking jobs, snooping for factions in corporate political fights, lawyers pursuing privacy-rights and First Amendment cases, and other parties with legitimate reasons to need an electronic locksmith.

SATAN

Security Administrator Tool for Analyzing Networks - A tool for remotely probing and identifying the vulnerabilities of systems on IP networks. A powerful freeware program which helps to identify system security weaknesses.

Secure Network Server

A device that acts as a gateway between a protected enclave and the outside world.

Secure Shell

A completely encrypted shell connection between two machines protected by a super long pass-phrase.

Security

A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.

Security Architecture

A detailed description of all aspects of the system that relate to security, along with a set of principles to guide the design. A security architecture describes how the system is put together to satisfy the security requirements.

Security Audit

A search through a computer system for security problems and vulnerabilities.

Security Countermeasures

Countermeasures that are aimed at specific threats and vulnerabilities or involve more active techniques as well as activities traditionally perceived as security

Security Domains

The sets of objects that a subject has the ability to access.

Security Features The security-relevant functions, mechanisms, and characteristics of AIS hardware and software.

Security Incident

Any act or circumstance that involves classified information that deviates from the requirements of governing security publications. For example, compromise, possible compromise, inadvertent disclosure, and deviation.

Security Kernel

The hardware, firmware, and software elements of a Trusted Computing Base that implement the reference monitor concept. It must mediate all accesses, be protected from modification, and be verifiable as correct.

Security Label

Piece of information that represents the sensitivity of a subject or object, such as its hierarchical classification (CONFIDENTIAL, SECRET, TOP SECRET) together with any applicable non-hierarchical security categories (e.g., sensitive compartmented information, critical nuclear weapon design information).

Security Level

The combination of a hierarchical classification and a set of non-hierarchical categories that represents the sensitivity of information.

Security Officer

The ADP official having the designated responsibility for the security of and ADP system

Security Perimeter

The boundary where security controls are in effect to protect assets.

Security Policies

The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Security Policy Model

A formal presentation of the security policy enforced by the system. It must identify the set of rules and practices that regulate how a system manages, protects, and distributes sensitive information.

Security Requirements

Types and levels of protection necessary for equipment, data, information, applications, and facilities.

Security Service

A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers.

Security Violation

An instance in which a user or other person circumvents or defeats the controls of a system to obtain unauthorized access to information contained therein or to system resources.

Server

A system that provides network service such as disk storage and file transfer, or a program that provides such a service. A kind of daemon which performs a service for the requester, which often runs on a computer other than the one which the server runs.

Signaling System 7 (SS-7)

A protocol used by phone companies. Has three basic functions: Supervising, Alerting and Addressing. Supervising monitors the status of a line or circuit to see if it is busy, idle, or requesting service. Alerting indicates the arrival of an incoming call. Addressing is the transmission of routing and destination signals over the network in the form of dial tone or data pulses.

Simple Network Management Protocol (SNMP)

Software used to control network communications devices using TCP/IP

Skipjack

An NSA-developed encryption algorithm for the Clipper chip. The details of the algorithm are unpublished.

Smurfing

A denial of service attack in which an attacker spoofs the source address of an echo-request ICMP (ping) packet to the broadcast address for a network, causing the machines in the network to respond en masse to the victim thereby clogging its network.

Snarf

To grab a large document or file for the purpose of using it with or without the author's permission.

Sneaker

An individual hired to break into places in order to test their security; analogous to tiger team.

Sniffer

A program to capture data across a computer network. Used by hackers to capture user id names and passwords. Software tool that audits and identifies network traffic packets. Is also used legitimately by network operations and maintenance personnel to troubleshoot network problems.

Spam

To crash a program by overrunning a fixed-site buffer with excessively large input data. Also, to cause a person or newsgroup to be flooded with irrelevant or inappropriate messages.

Special Information Operations (SIO)

Information Operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process. (DODD S-3600.1 of 9 Dec 96)

SPI

Secure Profile Inspector - A network monitoring tool for Unix, developed by the Department of Energy.

Spoofing

Pretending to be someone else. The deliberate inducement of a user or a resource to take an incorrect action. Attempt to gain access to an AIS by pretending to be an authorized user. Impersonating, masquerading, and mimicking are forms of spoofing.

SSL (Secure Sockets Layer)

A session layer protocol that provides authentication and confidentiality to applications.

Subversion

Occurs when an intruder modifies the operation of the intrusion detector to force false negatives to occur.

SYN Flood

When the SYN queue is flooded, no new connection can be opened.

[T]

TCP/IP

Transmission Control Protocol/Internetwork Protocol. The suite of protocols the Internet is based on.

tcpwrapper

A software tool for security which provides additional network logging, and restricts service access to authorized hosts by service.

Term Rule-Based Security Policy

A security policy based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users.

Terminal Hijacking

Allows an attacker, on a certain machine, to control any terminal session that is in progress. An attack hacker can send and receive terminal I/O while a user is on the terminal.

Threat

The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security.

Threat Agent

Methods and things used to exploit a vulnerability in an information system, operation, or facility; fire, natural disaster and so forth.

Threat Assessment

Process of formally evaluating the degree of threat to an information system and describing the nature of the threat.

Tiger

A software tool which scans for system weaknesses.

Tiger Team

Government and industry - sponsored teams of computer experts who attempt to break down the defenses of computer systems in an effort to uncover, and eventually patch, security holes.

Tinkerbell Program

A monitoring program used to scan incoming network connections and generate alerts when calls are received from particular sites, or when logins are attempted using certain ID's.

Topology

The map or plan of the network. The physical topology describes how the wires or cables are laid out, and the logical or electrical topology describes how the information flows.

Trace Packet

In a packet-switching network, a unique packet that causes a report of each stage of its progress to be sent to the network control center from each visited system element.

Traceroute

An operation of sending trace packets for determining information; traces the route of UDP packets for the local host to a remote host. Normally traceroute displays the time and location of the route taken to reach its destination computer.

Tranquillity A security model rule stating that the security level of an active object cannot change during the period of activity.

Tripwire

A software tool for security. Basically, it works with a database that maintains information about the byte count of files. If the byte count has changed, it will identify it to the system security manager.

Trojan Horse

An apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data.

Trusted Computer System Evaluation Criteria

(TCSEC) A system that employs sufficient hardware and software assurance measures to allow its use for simultaneous processing of a range of sensitive or classified information.

Trusted Computing Base (TCB)

The totality of protection mechanisms within a computer system including hardware, firmware, and software - the combination of which are responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system.

Trusted Network Interpretation

The specific security features, the assurance requirements and the rating structure of the Orange Book as extended to networks of computers ranging from isolated LANs to WANs.

TTY Watcher

A hacker tool that allows hackers with even a small amount of skill to hijack terminals. It has a GUI interface.

[V]

Vaccines

Program that injects itself into an executable program to perform a signature check and warns if there have been any changes.

Virus

A program that can "infect" other programs by modifying them to include a, possibly evolved, copy of itself.

Vulnerability

Hardware, firmware, or software flow that leaves an AIS open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

Vulnerability Analysis

Systematic examination of an AIS or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

[W]

WAIS

Wide Area Information Service - An Internet service that allows you to search a large number of specially indexed databases.

WAN

Wide Area Network. A physical or logical network that provides capabilities for a number of independent devices to communicate with each other over a common transmission-interconnected topology in geographic areas larger than those served by local area networks.

War Dialer

A program that dials a given list or range of numbers and records those which answer with handshake tones, which might be entry points to computer or telecommunications systems.

Worm

Independent program that replicates from machine to machine across network connections often clogging networks and information systems as it spreads.

Acceptable Risk is a concern that is acceptable to responsible management, due to the cost and magnitude of implementing controls / countermeasures..
Accreditation is synonymous with the term authorize processing. Accreditation is the authorization and approval granted to a major application or general support system to process in an operational environment. It is made on the basis of a certification by designated technical personnel that the system meets pre-specified technical requirements for achieving adequate system security. See also ***Authorize Processing, Certification*** and ***Designated Approving Authority.***
Adequate Security. Security implemented to fully meet the requirements put forth in public laws, Executive Branch directions, Federal standards, and agency-specific policies. Security will be implemented commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the Department operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost effective management, personnel, operational, and technical controls.
Asset is a major application, general support system, high impact program, physical plant, mission critical system, or a logically related group of systems.
Authorize Processing, Certification, and Designated Approving Authority. Authorize Processing occurs when management authorizes in writing a system based on an assessment of management, operational, and technical controls. By authorizing processing in a system the management official accepts the risks associated with it. See also ***Accreditation, Certification,*** and ***Designated Approving Authority.***
Automatic Data Processing (ADP) System - An assembly of computer hardware, firmware, and software configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, storing, and retrieving data with a minimum of human intervention.
Availability. Protection requires backup of system and information, contingency plans, disaster recovery plans, and redundancy. Examples of systems and information requiring availability protection are time-share systems, mission-critical applications, time and attendance, financial, procurement, or life-critical. ***Availability****:* A “requirement intended to assure that systems work promptly and service is not denied to authorized users”.
Awareness, Training, and Education includes (1) awareness programs set the stage for training by changing organizational attitudes towards realization of the importance of security and the adverse consequences of its failure; (2) the purpose of training is to teach people the skills that will enable

them to perform their jobs more effectively; and (3) education is more in-depth than training and is targeted for security professionals and those whose jobs require expertise in IT security.

Baseline - A set of critical observations or data used for a comparison or a control. A baseline indicates a cutoff point in the design and development of a configuration item beyond which configuration does not evolve without undergoing strict configuration control policies and procedures.

Bureau. Includes all independent offices within the Office of the Secretary as well as all organizations under the jurisdiction of the Assistant Secretaries even though the organization is titled other than "bureau".

Certification is synonymous with the term authorize processing. Certification is a major consideration prior to authorizing processing, but not the only consideration. Certification is the technical evaluation that establishes the extent to which a computer system, application, or network design and implementation meets a pre-specified set of security requirements. See also ***Accreditation*** and ***Authorize Processing.***

The ***Computer Security Act*** defines a *computer system* as "any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information: and includes computers: accessory equipment: software, firmware, and similar procedures and services, including support services." Applications are included in the definition of computer systems.

Computer Security: The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

Confidentiality: A requirement that private confidential information not be disclosed to unauthorized individuals.

Confidentiality Protection requires access controls such as user ID/passwords, terminal identifiers, restrictions on actions like read, write, delete, etc. Examples of confidentiality-protected information are personnel, financial, proprietary, trade secrets, internal agency, investigations, other federal agency, national resources, national security, and high or new technology under Executive Order or Act of Congress.

Configuration Accounting - The recording and reporting of configuration item descriptions and all departures from the baseline during design and production.

Configuration Audit - An independent review of computer software for the purpose of assessing compliance with established requirements, standards, and baselines.

Configuration Control - The process of controlling modifications to the system's design, hardware, firmware, software, and documentation which provides sufficient assurance the system is protected against the introduction of improper modification prior to, during, and after system implementation.

Configuration Control Board (CCB) - An established committee that is the final authority on all proposed changes to the ADP system.

Configuration Identification - The identifying of the system configuration throughout the design, development, test, and production tasks.

Configuration Item - The smallest component of hardware, software, firmware, documentation, or any of its discrete portions, which is tracked by the configuration management system.

Configuration Management - The management of changes made to a system's hardware, software, firmware, documentation, tests, test fixtures, and test documentation throughout the development and operational life of the system.

Critical Asset: An asset that supports national security, national economic security, and/or crucial public health and safety activities.

Descriptive Top-Level Specification (DTLS) - A top-level specification that is written in a natural language (e.g., English), an informal program design notation, or a combination of the two.

Designated Approving Authority (DAA) is the senior management official who has the authority to authorize processing (accredit) an automated information (major application) or (general support system) and accept the risk associated with the system.

Firmware - Equipment or devices within which computer programming instructions necessary to the performance of the device's discrete functions are electrically embedded in such a manner that they cannot be electrically altered during normal device operations.

Formal Security Policy Model - An accurate and precise description, in a formal, mathematical language, of the security policy supported by the system.

Formal Top-Level Specification - A top-level specification that is written in a formal mathematical language to allow theorems showing the correspondence of the system specifications to its formal requirements to be hypothesized and formally proven.

General Support System is an interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

Granularity - The relative fineness or coarseness by which a mechanism can be adjusted. The phrase "the granularity of a single user" means the access control mechanism can be adjusted to include or exclude any single user.

Hardware - The electric, electronic, and mechanical equipment used for processing data.

Individual Accountability requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.

Informal Security Policy Model - An accurate and precise description, in a natural language (e.g., English), of the security policy supported by the system.

Information Owner is responsible for establishing the rules for appropriate use and protection of the data/information. The information owner retains that responsibility even when the data/information are shared with other organizations.

Information Technology Facility. An organized grouping of personnel, hardware, software, and physical facilities, a primary function of which is the operation of information technology.

Information Technology Installation. One or more computer or office automation systems including related telecommunications, peripheral or storage units, central processing units, and operating and support system software. Information technology installations may range from information technology facilities, such as large centralized computer centers, to individual stand-alone microcomputers such as personal computers, or workstations.

Information Technology Resources. Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the Department. The term "information technology resources" includes computers, telecommunications equipment, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

Information Technology System. An organized combination of ADP equipment, software, and established methods and procedures designed to collect, process, and/or communicate data or information for the purposes of supporting specific administrative, mission, or program requirements. This includes the areas of application systems, data bases, and management information systems.

***Information Technology Security*.** The management controls and safeguards designed to protect IT resources and safeguard governmental assets and individual privacy.

Integrity*:* In lay usage, information has integrity when it is timely, accurate, complete, and consistent. However, computers are unable to provide or protect all of these qualities. Therefore, in the computer security field, integrity is often discussed more narrowly as having two facets *data integrity* and *system integrity*. "Data integrity is a requirement that information and programs are changed only in a specified and authorized manner". (National Research Council, Computers at Risk, (Washington, DC: National Academy Press, 1994), p.54) System integrity is a requirement that a system " perform its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system". (National Computer Security Center, Pub. NCSC-TG-004-88) The definition of integrity has been, and continues to be, the subject of many debates among computer security experts.

Major Application (a) is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

***Major Application (b)*.** An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

Major Application (c). Or software system has no platform, but utilizes the services of another system's platform and communications is also considered sensitive. If the partitioning (or boundaries) of the system are logically or functionally defined. A major application requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. The system should be defined such that, as a whole, there is a completed product such as a report or a completed transaction

***Management Control*.** Focuses on the management of IT computer security systems and the risk management of those systems.

Management Control Measures. Types of control measures which shall be consistent with the need for protection of the major application or general support system. For more detail on management controls, see NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook".

Risk Assessment and Management. OMB Circular A-130 no longer requires the preparation of a formal risk analysis. It does, however, require an assessment of risk as part of a risk-based approach to determining adequate, cost-effective security for a system. The methods used to assess the nature and level of risk to the system should include a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards.

Material Weakness or significant weakness is used to identify control weaknesses that pose a significant risk or a threat to the operations and/or assets of an audited entity. "Material weakness" is a very specific term that is defined one way for financial audits and another way for weaknesses reported under the Federal Managers Financial Integrity Act of 1982. Such weaknesses may be identified by auditors or by management.

Mission Essential Infrastructure Assets **(MEIA)** can be defined as the critical organizations, personnel, systems, and facilities that are absolutely required in order to provide the inputs and outputs necessary to support the core processes essential to accomplishing the Interior's core missions. The Interior's MEIA includes those IT system assets that are internal (Departmentally controlled) and external (non-Departmentally controlled) cyber-based and non-cyber-based.

Networks include communication capability that allows one user or system to connect to another user or system and can be part of a system or a separate system. Examples of networks include local area network or wide area networks, including public networks such as the Internet.

Operational Controls address security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).

Policy a document that delineates the security management structure and clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance.

Procedures a document that focuses on the security control areas and management's position.

Risk is the possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.

Risk Assessment. An evaluation of IT assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events. A risk assessment identifies potential threats and their probability of occurrence and proposes safeguards to combat these threats. Provides management with information on which to base decisions, (e.g., whether it is best to prevent the occurrence of a situation), to contain the effect it may have, or simply to recognize that a potential for loss exists.

Risk Management is the ongoing process of assessing the risk to automated information resources and information, as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.

Rules of Behavior are the rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of Federal government equipment, assignment and limitation of system privileges, and individual accountability.

Security Specifications. A detailed description of the safeguards required to protect a sensitive system/application.

Sensitive System. A system containing information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of the Department of the Interior to accomplish its mission, e.g., proprietary information, information about individuals requiring protection under the Privacy Act, and information not releasable under the Freedom of Information Act. (For more information, refer to 383 DM 1-15.)

Sensitive Information refers to information whose loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs or the privacy to which individuals are entitled. However, please bear in mind that an IT system is considered *"sensitive"* if it meets any one of the following three tests:

- *Confidentiality* – the system contains information that requires protections from unauthorized disclosure.
- *Integrity* – the system contains information that must be protected from unauthorized, unanticipated or unintentional modification.
- *Availability* – the system contains information or provides services which must be available on a timely basis to meet mission requirements or to avoid substantial losses

Sensitivity an information technology environment consists of the system, data, and applications that must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and/or availability which is determined by an evaluation of the sensitivity of the information processed, the relationship of the system to the organizations mission, and the economic value of the system components.

Software - Various programming aids that are frequently supplied by the manufacturers to facilitate the purchaser's efficient operation of the equipment. Such software items include various assemblers, generators, subroutine libraries, compilers, operating systems, and industry application programs.

System is a generic term used for briefness to mean either a major application or a general support system.

System Operational Status is either (1) Operational - system is currently in operation, (2) Under Development - system is currently under design, development, or implementation, or (3) Undergoing a Major Modification - system is currently undergoing a major conversion or transition.

Technical Controls consist of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.

Threat (a) is an event or activity, deliberate or unintentional, with the potential for causing harm to an IT system or activity.

Threat (b***):*** Any circumstance or event that could harm a critical asset through unauthorized access, through unauthorized access, compromised of data integrity, denial or disruption of service, or physical destruction or impairment.

Tools - The means for achieving an end result. The tools referred to in this guideline are documentation, procedures, and the organizational body, i.e., the CCB, which all contribute to achieving the control objective of configuration management.

Trusted Computing Base (TCB) - The totality of protection mechanisms within a computer system -- including hardware, firmware, and software -- the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy.

Vulnerability is a flaw or weakness that may allow harm to occur to an IT system or activity.

***Vulnerability Assessment*:** An examination of the ability of a system or application, including current security procedures and controls, to withstand assaults.   A vulnerability assessment may be used to (1) identify weakness that could be exploited; and (2) predict the effectiveness of additional security measures in protecting information resources from attack.
***Vulnerability Audit**:* The process of identify and documenting specific vulnerabilities in critical information in critical information systems.

- A -

Abuse of Privilege: When a user performs an action that they should not have, according to organizational policy or law. /\

Access: The ability to enter a secured area. The process of interacting with a system. Used as either a verb or a noun. /\

Access Authorization: Permission granted to users, programs or workstations. /\

Access Control: A set of procedures performed by hardware, software and administrators to monitor access, identify users requesting access, record access attempts, and grant or deny access. /\

Access Sharing: Permitting two or more users simultaneous access to file servers or devices. /\

Alphanumeric Key: A sequence of letters, numbers, symbols and blank spaces from one to 80 characters long. /\

ANSI: The American National Standards Institute. Develops standards for transmission storage, languages and protocols. Represents the United States in the ISO (International Standards Organization). /\

Application Level Gateway [Firewall]: A firewall system in which service is provided by processes that maintain complete TCP connection state and sequencing. Application level firewalls often re-address traffic so that outgoing traffic appears to have originated from the firewall, rather than the internal host. /\

Application Logic: The computational aspects of an application, including a list of instructions that tells a software application how to operate. /\

Audit: The independent collection of records to access their veracity and completeness. /\

Audit Trail: An audit trail may be on paper or on disk. In computer security systems, a chronological record of when users log in, how long they arc engaged in various activities, what they were doing, whether any actual or attempted security violations occurred. /\

Authenticate: In networking, to establish the validity of a user or an object (i.e. communications server). /\

Authentication: The process of establishing the legitimacy of a node or user before allowing access to requested information. During the process, the user enters a name or account number (identification) and password (authentication). /\

Authentication Tool: A software or hand-held hardware "key" or "token" utilized during the user authentication process. See key and token. /\

Authentication Token: A portable device used for authenticating a user. Authentication tokens operate by challenge/response, time-based code sequences, or other techniques. This may include paper-based lists of one-time passwords. /\

Authorization: The process of determining what @ of activities are permitted. Usually, authorization is in the context of authentication. Once you have authenticated a user, the user may be authorized different @s of access or activity. /\

Availability: The portion of time that a system can be used for productive work, expressed as a percentage. /\

- B -

Back Door: An entry point to a program or a system that is hidden or disguised, often created by the software's author for maintenance. A certain sequence of control characters permits access to the system manager account. If the back door becomes known, unauthorized users (or malicious software) can gain entry and cause damage. /\

Bandwidth: Capacity of a network or data connection, often measured in kilobits/second (kbps) for digital transmissions. /\

Bastion Host: A system that has been hardened to resist attack at some critical point of entry, and which is installed on a network in such a way that it is expected to come under attack. Bastion hosts are often components of firewalls, or may be 'outside" Web servers or public access systems. Generally, a bastion host is running some form of general purpose operating system (e.g., LNIX, VMS, WNT, etc.) rather than a ROM-based or firmware operating system. /\

Biometric Access Control: Any means of controlling access through human measurements, such as fingerprinting and voiceprinting. /\

Business-Critical Applications: The vital software needed to run a business, whether custom-written or commercially packaged, such as accounting/finance, ERP, manufacturing, human resources, sales databases, etc. /\

- C -

CERT: The Computer Emergency Response Team was established at Carnegie-Mellon University after the 1988 Internet worm attack. /\

Challenge/Response: A security procedure in which one communicator requests authentication of another communicator, and the latter replies with a pre-established appropriate reply. /\

Chroot: A technique under UNIX whereby a process is permanently restricted to an isolated subset of the file system. /\

Client/Device: Hardware that retrieves information from a server. /\

Clustering: Group of independent systems working together as a single system. Clustering technology allows groups of servers to access a single disk array containing applications and data. /\

Coded File: In encryption, a coded file contains unreadable information. /\

Combined Evaluation: Method using proxy and state or filter evaluations as allowed by administrator. [See State Full Evaluation]. /\

Communications Server: Procedures designed to ensure that telecommunications messages maintain their integrity and are not accessible by unauthorized individuals. /\

Computer Security: Technological and managerial procedures applied to computer systems to ensure the availability, integrity and confidentiality of information managed by the computer system. /\

Computer Security Audit: An independent evaluation of the controls employed to ensure appropriate protection of an organization's information assets. /\

Cryptographic Checksum: A one-way function applied to a file to produce a unique "fingerprint" of the file for later reference. Checksum systems are a primary means of detecting file system tampering on UNIX. /\

- D -

Data Driven Attack: A form of attack in which the attack is encoded in innocuous-seeming data which is executed by a user or other software to implement an attack. In the case of firewalls, a data driven attack is a concern since it may get through the fir-firewall in data form and launch an attack against a system behind the firewall. /\

Data Encryption Standard: An encryption standard developed by EBM and then tested and adopted by the National Bureau of Standards. Published in 1977, the DES standard has proven itself over nearly 20 years of use in both government and private sectors. /\

Decode: Conversion of encoded text to plain text through the use of a code. /\

Decrypt: Conversion of either encoded or enciphered text into plaintext. /\

Dedicated: A special purpose device. Although it is capable of performing other duties, it is assigned to only one. /\

Defense in Depth: The security approach whereby each system on the network is secured to the greatest possible degree. May be used in conjunction with firewalls. /\

DES: Data encryption standard. /\

DNS Spoofing: Assuming the DNS name of another system by either corrupting the name service cache of a victim system, or by compromising a domain name server for a valid domain. /\

Dual Homed Gateway: 1) A system that has two or more network interfaces, each of which is connected to a different network. In firewall configurations, a dual homed gateway usually acts to block or filter some or all of the traffic trying to pass between the networks. 2) A firewall implement without the use of a screening router. /\

- E -

E-mail Bombs: Code that when executed sends many messages to the same address(s) for the purpose of using up disk space and/or overloading the E-mail or web server. /\

Encrypting Router: See Tunneling Router and Virtual Network Perimeter. /\

Encryption: The process of scrambling files or programs, changing one character string to another through an algorithm (such as the DES algorithm). /\

End-to-End Encryption: Encryption at the point of origin in a network, followed by decryption at the destination. /\

Environment: The aggregate of external circumstances, conditions and events that affect the development, operation and maintenance of a system. /\

ERP: An acronym for Enterprise Resource Planning systems that permit organizations to manage resources across the enterprise and completely integrate manufacturing systems. /\

Extranet: "Extranet" refers to extending the LAN via remote or Internet access to partners outside your organization such as frequent suppliers and purchasers. Such relationships should be over authenticated link to authorized segments of the LAN and are frequently encrypted for privacy." /\

- F -

Fat Client: A computing device, such as a PC or Macintosh, that includes an operating system, RAM, ROM, a powerful processor and a wide range of installed applications that can execute on the desktop or 100% on the server under a Server-based Computing architecture. Fat clients can operate in a Server-based Computing environment. /\

Fault Tolerance: A design method that ensures continued systems operation in the event of individual failures by providing redundant system elements. /\

Firewall: A system or combination of systems that enforces a boundary between two or more networks. /\

Flooding programs: Code which when executed will bombard the selected system with requests in an effort to slow down or shut down the system. /\

Anonymous FTP: A guest account which allows anyone to login to the FTP Server. It can be a point to begin access on the host server. /\

- G -

Gateway: A bridge between two networks. /\

Generic Utilities: General purpose code and devices; i.e., screen grabbers and sniffers that look at data and capture information like passwords, keys and secrets. /\

Global Security: The ability of an access control package to permit protection across a variety of mainframe environments, providing users with a common security interface to all. /\

Granularity: The relative fineness or coarseness by which a mechanism can be adjusted. /\

- H -

Hack: Any software in which a significant portion of the code was originally another program. /\

Hacker: Those intent upon entering an environment to which they are not entitled entry for whatever purpose [entertainment, profit, theft, prank, etc.]. Usually iterative techniques escalating to more advanced methodologies and use of devices to intercept the communications property of another. /\

Host-based Security: The technique of securing an individual system from attack. Host-based security is operating system and version dependent. /\

Hot Standby: A backup system configured in such a way that it may be used if the system goes down. /\

Hybrid Gateways: An unusual configuration with routers that maintain the complete state of the TCP/IP connections or examine the traffic to try to detect and prevent attack [may involve baston host]. If very complicated it is difficult to attach; and, difficult to maintain and audit. /\

- I -

ICA: An acronym for Citrix's Independent Computing Architecture, a three-part Server-based Computing technology that separates an application's logic from its user interface and allows 100% application execution on the server. /\

IETF: The Internet Engineering Task Force, a public forum that develops standards and resolves operational issues for the Internet. IETF is purely voluntary. /\

Information Systems Technology: The protection of information assets from accidental or intentional but unauthorized disclosure, modification, or destruction, or the inability to process that information. /\

Insider Attack: An attack originating from inside a protected network. /\

Internet (The Beginning): The Internet had its roots in early 1969 when the ARPANET was formed. ARPA stands for Advanced Research Projects Agency (which was part of the U.S. Department of Defense). One of the goals of ARPANET was research in distributed computer systems for military purposes. The first configuration involved four computers and was designed to demonstrate the feasibility of building networks using computers dispersed over a wide area. The advent of OPEN networks in the late 1980's required a new model of communications. The amalgamation of many types of systems into mixed environments demanded better translator between these operating systems and a non-proprietary approach to networking in general. Telecommunications Protocol/Internet Protocol {TCP/IP) provided the best solutions to this. /\

Internet (TOM): A web of different, intercommunicating networks funded by both commercial and government organizations. It connects networks in 40 countries. No one owns or runs the Internet. There are thousands of enterprise networks connected to the Internet, and there are millions of users, with thousands more joining every day. /\

Intrusion Detection: Detection of break-ins or break-in attempts either manually via software expert systems that operate on logs or other information available on the network. /\
IP Sniffing: Stealing network addresses by reading the packets. Harmful data is then sent stamped with internal trusted addresses. /\
IP Spoofing: An attack whereby an active, established, session is intercepted and co-opted by the attacker. EP Splicing attacks may occur after an authentication has been made, permitting the attacker to assume the role of an already authorized user. Primary protections against IP Splicing rely on encryption at the session or network layer. /\
IP Spoofing: An attack whereby a system attempts to illicitly impersonate another system by using its EP network address. /\
ISO: International Standards Organization sets standards for data communications. /\
ISSA: Information Systems Security Association. /\
- J -

[No Entries] /\
- K -
Key: In encryption, a key is a sequence of characters used to encode and decode a file. You can enter a key in two formats: alphanumeric and condensed (hexadecimal). In the network access security market, "key" often refers to the "token," or authentication tool, a device utilized to send and receive challenges and responses during the user authentication process. Keys may be small, hand-held hardware devices similar to pocket calculators or credit cards, or they may be loaded onto a PC as copy-protected, software. /\
- L -
Least Privilege: Designing operational aspects of a system to operate with a minimum amount of system privilege. This reduces the authorization level at which various actions are performed and decreases the chance that a process or user with high privileges may be caused to perform unauthorized activity resulting in a security breach. /\
Local Area Network (LAN): An interconnected system of computers and peripherals, LAN users share data stored on hard disks and can share printers connected to the network. /\
Logging: The process of storing information about events that occurred on the firewall or network. /\
Log Processing: How audit logs are processed, searched for key events, or summarized. /\
Log Retention: How long audit logs are retained and maintained. /\
- M -
Mobile Code: A program downloaded from the internet that runs automatically on a computer with little or no user interaction.
Multi-User: The ability for multiple concurrent users to log on and run applications from a single server. /\
- N -
Network Computer (NC): A "thin" client hardware device that executes applications locally by downloading them from the network. NCs adhere to a specification jointly developed by Sun, IBM, Oracle, Apple and Netscape. They typically run Java applets within a Java browser, or Java applications within the Java Virtual Machine. /\
Network Computing Architecture: A computing architecture in which components are dynamically downloaded from the network into the client device for execution by the client. The Java programming language is at the core of network computing. /\
Network-Level Firewall: A firewall in which traffic is examined at the

network protocol packet level. /\

Network Worm: A program or command file that uses a computer network as a means for adversely affecting a system's integrity, reliability or availability, A network worm may attack from one system to another by establishing a network connection. It is usually a self-contained program that does not need to attach itself to a host file to infiltrate network after network. /\

- O -

One-Time Password: In network security, a password issued only once as a result of a challenge-response authentication process. Cannot be "stolen" or reused for unauthorized access. /\

Operating System: System software that controls a computer and its peripherals. Modern operating systems such as Windows 95 and NT handle many of a computer’s basic functions. /\

Orange Book: The Department of Defense Trusted Computer System Evaluation Criteria. It provides information to classify computer systems, defining the degree of trust that may be placed in them. /\

- P -

Password: A secret code assigned to a user. A@ known by the computer system. Knowledge of the password associated with the user ID is considered proof of authorization. (See One-Time Password.) /\

Performance: A major factor in determining the overall productivity of a system, performance is primarily tied to availability, throughput and response time. /\

Perimeter-based Security: The technique of securing a network by controlling access to all entry and exit points of the network. /\

PIN: In computer security, a personal identification number used during the authentication process. Known only to the user. (See Challenge/Response, Two-Factor Authentication.) /\

Policy: Organizational-level rules governing acceptable use of computing resources, security practices, and operational procedures. /\

Private Key: In encryption, one key (or password) is used to both lock and unlock data. Compare with public key. /\

Protocols: Agreed-upon methods of communications used by computers. /\

Proxy: 1) A method of replacing the code for service applications with an improved version that is more security aware. Preferred method is by "service communities", i.e. Oracle, rather than individual applications. Evolved from socket implementations. 2) A software agent that acts on behalf of a user. Typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination. /\

Public Key: In encryption a two-key system in which the key used to lock data is made public, so everyone can "lock." A second private key is used to unlock or decrypt. /\

- Q -

[No Entries] /\

- R -

Remote Access: The hookup of a remote computing device via communications lines such as ordinary phone lines or wide area networks to access network applications and information. /\

Remote Presentation Services Protocol: A protocol is a set of rules and procedures for exchanging data between computers on a network. A remote presentation services protocol transfers user interface, keystrokes, and mouse movements between a server and client. /\

Risk Analysis: The analysis of an organization's information resources, existing controls and computer system vulnerabilities. It establishes a potential level of damage in dollars and/or other assets. /\

Rogue program: Any program intended to damage programs or data. Encompasses malicious Trojan Horses. /\

RSA: A public key cryptosystem named by its inventors, Rivest, Shamir and Adelman, who hold the patent. /\

- S -

Scalability: The ability to expand a computing solution to support large numbers of users without impacting performance. /\

Screened Host Gateway: A host on a network behind a screening router. The degree to which a screened host may be accessed depends on the screening rules in the router. /\

Screened Subnet: An isolated subnet created behind a screening router to protect the private network. The degree to which the subnet may be accessed depends on the screening rules in the router. /\

Screening Router: A router configured to permit or deny traffic using filtering techniques; based on a set of permission rules installed by the administrator. A component of many firewalls usually used to block traffic between the network and specific hosts on an IP port level. Not very secure; used when "speed" is the only decision criteria. /\

Server: The control computer on a local area network that controls software access to workstations, printers and other parts of the network. /\

Server-based Computing: An innovative, server-based approach to delivering business-critical applications to end-user devices, whereby an application’s logic executes on the server and only the user interface is transmitted across a network to the client. Its benefits include single-point management, universal application access, bandwidth-independent performance, and improved security for business applications. /\

Server Farm: A group of servers that are linked together as a ‘single system image’ to provide centralized administration and horizontal scaleability. /\

Session Shadowing: A feature of Citrix WinFrame and MetaFrame that allows administrators and technical support staff to remotely join or take control of a user’s session for diagnosis, support and training. /\

Session Stealing: See IP Splicing. /\

Single-Point Control: Helps reduce the total cost of application ownership by enabling applications and data to be deployed, managed and supported at the server. Single-point control enables application installations, updates and additions to be made once, on the server, which are then instantly available to users anywhere. /\

Smart Card: A credit-card-sized device with embedded microelectronics circuitry for storing information about an individual. This is not a key or token, as used in the remote access authentication process. /\

Social Engineering: An attack based on deceiving users or administrators at the target site. Social engineering attacks are typically carried out by telephoning users or operators and pretending to be an authorized user, to attempt to gain illicit access to systems. /\

State Full Evaluation: Methodology using mixture of proxy or filtering technology intermittently depending upon perceived threat [and/or need for "speed"]. /\

- T -

TCO: Total Cost of Ownership, a model that helps IT professionals understand and manage the budgeted (direct) and unbudgeted (indirect) costs incurred for acquiring, maintaining and using an application or a computing system. TCO normally includes training, upgrades, and administration as well as the purchase price. Lowering TCO through single-point control is a key benefit of Server-based Computing. /\

Thin Client: A low-cost computing device that works in a server-centric computing model. Thin clients typically do not require state-of-the-art, powerful processors and large amounts of RAM and ROM because they access applications from a central server or network. Thin clients can operate in a Server-based Computing environment. /\

Token: A "token" is an authentication too, a device utilized to send and receive challenges and responses during the user authentication process. Tokens may be small, hand-held hardware devices similar to pocket calculators or credit cards. See key. /\

Trojan Horse: 1) Any program designed to do things that the user of the program did not intend to do or that disguises its harmful intent. 2) Program that installs itself while the user is making an authorized entry; and, then are used to break-in and exploit the system. /\

Tunneling Router: A router or system capable of routing traffic by encrypting it and encapsulating it for transmission across an untrusted network, for eventual de-encapsulation and decryption. /\

Turn Commands: Commands inserted to forward mail to another address for interception. /\

Two-Factor Authentication: Two-factor authentication is based on something a user knows (factor one) plus something the user has (factor two). In order to access a network, the user must have both "factors" - just as he/she must have an ATM card and a Personal Identification Number (PIN) to retrieve money from a bank account, In order to be authenticated during the challenge/response process, users must have this specific (private) information. /\

- U -

User: Any person who interacts directly with a computer system. /\

User ID: A unique character string that identifies users. /\

User Identification: User identification is the process by which a user identifies himself to the system as a valid user. (As opposed to authentication, which is the process of establishing that the user is indeed that user and has a right to use the system.) /\

User Interface: The part of an application that the user works with. User interfaces can be text-driven, such as DOS, or graphical, such as Windows. /\

- V -

Virtual Network Perimeter: A network that appears to be a single protected network behind firewalls, which actually encompasses encrypted virtual links over untrusted networks. /\

Virus: A self-replicating code segment. Viruses may or may not contain attack programs or trapdoors. /\

- W -

Windows-Based Terminal (WBT): A fixed-function thin client device that connects to a Citrix WinFrame or MetaFrame server and Terminal Server to provide application access. The key differentiator of a WBT from other thin devices is that all application execution occurs on the server; there is no downloading or local processing of applications at the client. /\

Windows NT 4.0, Terminal Server Edition: A multi-user operating system for Windows NT 4.0 from Microsoft, formerly called "Hydra." /\

- XYZ -

Y2K: An acronym for the Year 2000 Problem that involves three issues - two-digit data storage, leap year calculations and special meanings for dates. /\